



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,588	08/07/2001	Thomas E. Tahan	5181-75900	2724
7590	02/22/2005			EXAMINER
Rory D. Rankin Conley, Rose, & Tayon, P.C. P.O. Box 398 Austin, TX 78767			SCHUBERT, KEVIN R	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/923,588	TAHAN, THOMAS E	
	<b>Examiner</b> Kevin Schubert	<b>Art Unit</b> 2137	

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 07 August 2001.

2a)  This action is FINAL.                    2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## **Disposition of Claims**

4)  Claim(s) 1-51 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5)  Claim(s) \_\_\_\_\_ is/are allowed.  
6)  Claim(s) 1-51 is/are rejected.  
7)  Claim(s) \_\_\_\_\_ is/are objected to.  
8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 07 August 2001 is/are: a)  accepted or b)  objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892) 4)  Interview Summary (PTO-413)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948) Paper No(s)/Mail Date. \_\_\_\_.  
3)  Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 01042002, 01222003. 5)  Notice of Informal Patent Application (PTO-152)  
6)  Other: \_\_\_\_.

Art Unit: 2137

**DETAILED ACTION**

Claims 1-51 have been considered. Claims 1-51 are drawn to a similar system as that of Tahan, U.S. Patent No. 6,760,330. To avoid double patenting, a statement of common ownership needs to be filed.

5

***Claim Objections***

Claims 8,25, and 42 are objected to because the claims are not grammatically correct. The examiner assumes the claim should read "said second action comprises changing said PCS to a second PCS in response to detecting said first rule **and** includes forwarding said first data packet". Appropriate 10 correction is required.

***Claim Rejections - 35 USC § 103***

Claims 1-51 are rejected under 35 U.S.C. 103(c) as being an obvious type double patenting of Tahan, U.S. Patent No. 6,760,330. The specifications of the instant application and U.S. Patent No. 15 6,760,330 are the same and the claims are drawn to minor, obvious modifications such as changing a MCN node to a firewall.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for 20 the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

30

Art Unit: 2137

Claims 1-2,5-10,12,15-16,18-19,22-27,29,32-33,35-36,39-44,46, and 49-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Bots, U.S. Patent No. 6,226,748.

As per claims 1,18, and 35, the applicant discloses a method of controlling information flow

5 through a firewall comprising the following limitations which are met by Bots:

- a) determining an incoming packet community set (PCS) of a first data packet received on an interface of said firewall (Col 7, lines 1-6);
- b) discarding said first data packet in response to detecting said PCS is not a subset of an interface community set (IFCS) of said interface (Col 8, lines 2-4);
- 10 c) processing said first data packet in response to detecting said PCS is a subset of said IFCS (Col 7, lines 20-24);

Both the applicant and Bots disclose methods for controlling information flow through a network and a firewall. The applicant discloses the use of calculating a packet community set at a receiving interface and an outgoing interface. Bots discloses the use of determining a virtual private network group 15 at a receiving interface, a first VPNU, and an outgoing interface, a second VPNU. Additionally, Bots discloses that the VPN unit may comprise a firewall (Col 9, lines 21-24).

Regarding part a), the first VPNU receives a data packet and determines the incoming PCS. The PCS in Bots' system is the virtual private network group which is determined by evaluating the packet in light of look up tables which specify whether the source and destination addresses are members of a 20 particular group and can therefore communicate with each other.

Regarding parts b) and c), if the first VPNU determines that the PCS of the data packet is a subset of the IFCS of the VPNU, the first VPNU processes the data packet according to special rules of encryption, authentication, and compression which allow the second VPNU, or the outgoing interface, to process the data as a member of a particular group which has the compression, encryption, and 25 authentication characteristics that were performed on it by the first VPNU. The IFCS is set of virtual private network groups in the table on the VPN units which specify which groups the VPN units interface with (Col 8, lines 2-4).

Art Unit: 2137

Regarding claims 18 and 35, the use of a CIB will be disclosed in the rejection for claim 15, and the use of communication between a first and second computer can be seen in Fig 2 (for example communication between 211 and 201).

5 As per claims 2,10,19,27,36, and 44, the applicant discloses the method of claims 1,9,18,26,35, and 43, which are met by Bots (see above), with the following limitation which is also met by Bots:

Wherein said determining comprises determining a source network address community set (NACS) of said first data packet (Col 6, lines 34-38; Col 7, lines 1-6).

10 The source and destination network address community sets are represented by the virtual private network group, which specifies which source and destination addresses are able to communicate with each other. As cited by Bots, "it is determined whether or not the source and destination addresses for the data packet are both members of the same VPN group" (Col 7, lines 1-6). Thus, each group comprises a source network address community set of source addresses which are members of the group and a destination community set of destination addresses which are members of the group.

15

As per claims 5,22, and 39, the applicant describes the method of claims 1,18, and 35, which are met by Bots (see above), with the following limitation which is also met by Bots:

Wherein said processing comprises matching said first data packet to a first rule of a plurality of rules of said firewall (Col 7, lines 20-24);

20 As described in the lines referenced above, if the data packet is verified as belonging to a group (PCS) in the groups which the VPNU serves (IFCS), it is processed according to a number of rules based on the particular group of the data packet. These rules are authentication, compression, and encryption rules which allow the second VPNU to authenticate the data packet and calculate the outgoing or second PCS.

25

As per claims 6,23, and 40, the applicant describes the method of claims 5,22, and 39, which are anticipated by Bots (see above), with the following limitation which is also met by Bots:

Art Unit: 2137

Wherein said first rule includes a PCS attribute, and wherein said processing further comprises performing a first action in response to detecting said PCS of said first data packet does not match said PCS attribute, and wherein said processing further comprises performing a second action in response to detecting said PCS of said first data packet matches said PCS attribute (Col 2, lines 55-65; Abstract)

5 As described above, the rules include attributes of the particular groups (PCS identities) such as specific compression, encryption, and authentication techniques which allow the VPNU to authenticate the data packet. If the second VPNU determines that the first data packet does not match the PCS attribute(s), it is not processed and it is discarded because the system is designed to only allow communication between proper parties (Col 8, lines 2-4). If the second VPNU determines that the first 10 data packet does match the PCS attribute(s), a second action is performed as the processing continues.

As per claims 7,24, and 41, the applicant describes the method of claims 6,23, and 40, which are met by Bots (see above), with the following limitation which is also met by Bots:

Wherein said first action comprises discarding said first data packet (Col 8, lines 2-4);  
15 The VPN units maintain lookup tables for identifying the members of the VPN groups (Col 6, lines 34-36), and communication is only allowed between members of the group.

As per claims 8,25, and 42, the applicant describes the method of claims 6,23, and 40, which are met by Bots (see above), with the following limitation which is also met by Bots:

20 Wherein said second action comprises changing said PCS to a second PCS in response to detecting said first rule includes forwarding said first data packet, wherein said second PCS is indicated by said first rule (Col 6, lines 41-46);

A second or outgoing PCS is evaluated on the second VPNU if the rules which were put on the data packet are recognized by the second VPNU. The second PCS is used to determine whether the 25 data packet can pass to its destination. The second PCS is indicated by the rule or rules because the virtual private network group, or second PCS, is ensured for authentication by the particular rules placed

Art Unit: 2137

on the data packet (Col 6, lines 37-48). If the second PCS or virtual private network group is one in which the second VPNU interfaces with, the first data packet is forwarded to its destination.

As per claims 9,26, and 43, the applicant describes the method of claims 8,25, and 43, which are 5 met by Bots (see above), with the following limitations which are also met by Bots:

- a) comparing said second PCS with a destination community set of said first data packet (Col 7, line 56 to Col 8, line 4);
- b) discarding said first data packet in response to detecting said second PCS is not a subset of said destination community set (Col 7, line 56 to Col 8, line 4);
- 10 c) processing said first data packet in response to detecting said second PCS is a subset of said destination community set (Col 7, line 56 to Col 8, line 4).

Regarding part a), the second PCS is the outgoing PCS (group) determined at the second VPN unit from the compression, encryption, authentication rules. The destination community set comprises the destinations the packet can be sent to. Referring to the Bots' drawings, 320 of Fig 3 represents the 15 first PCS (or VPN group) being calculated on the first VPNU and 420 of Fig 4 represents the second PCS (or VPN group) being calculated on the second VPNU.

Regarding part c), the destination community set is the set of destination addresses for the VPN group. The set of destination addresses is the same as the set of source addresses because the group includes information about which addresses are able to communicate with each other. Thus, the second 20 PCS, or VPN group, the source and destination addresses are a member of is the same as the destination community set. Since a set is a subset of itself, the second PCS is a subset of the destination community set.

As per claims 12,29, and 46, the applicant describes the method of claims 9,26, and 43, which 25 are met by Bots (see above), with the following limitations which are also met by Bots:

Art Unit: 2137

a) transmitting said first data packet via an output interface of said firewall in response to detecting said second PCS is a subset of the interface community set (IFCS) of said output interface (Col 6, lines 34-46);

5 b) discarding said first data packet in response to detecting said second PCS is not a subset of said IFCS (Col 8, lines 2-4);

Regarding part a), the second PCS identifies a user into a particular virtual private network group (Col 6, lines 34-36) in the second VPN unit. The interface community set is the set of all groups for which the second VPN unit communicates with. As described in the lines referenced above and (Col 7, lines 45-47), the VPN units interface with more than one virtual private network group. The first data packet is 10 transmitted to an end user if it is determined that it is in a group which the VPN unit serves. If the identified group is not one which the VPNU supports, it is discarded (Col 8, lines 2-4). Also, the use of a firewall as being configured into the VPN unit is disclosed by Bots (Col 9, lines 21-24).

15 As per claims 15,32, and 49, the applicant describes the method of claims 1,18, and 35, which is met by Bots (see above), with the following limitation which is also met by Bots:

Further comprising consulting a community information base (CIB) (Col 2, lines 62-65);

20 The community information base corresponds to lookup tables on the VPN units, which identify members of a group by their network addresses, provide services such as compression and encryption for authentication purposes, and include information corresponding to the VPN unit interfaces which allow the compression, encryption, and authentication rules of one VPN unit to be recognized by another.

As per claims 16,33, and 50, the applicant describes the method of claims 15,32, and 49, which are met by Bots (see above), with the following limitation which is also met by Bots:

25 Wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces (Col 2, lines 62-65);

See the rejection for claim 15 for more detail on the information in the lookup tables or CIB.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

5 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10

Claims 3,11,20,28,37, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of McNeill, U.S. Patent No. 6,167,052.

15 As per claims 3,11,20,28,37, and 45, the applicant discloses the method of claim 1,9,18,26,35, and 43, which are anticipated by Bots (see above), with the following additional limitation which is met by McNeill.

Wherein said determining comprises determining a source network service community set (NSCS) of said first data packet (McNeill: Abstract);

20 The applicant describes the NSCS as identifying the source and destination by link layer addressing or a similar layering protocol (Applicant: Page 26). Bots discloses all the limitations of claims 1,9,18,26,35, and 43 and the use of identifying a source by its address, but fails to disclose the use of determining a source by link layer addressing or similar layering protocol. McNeill discloses a system similar to Bots' and the applicant's in which connectivity is established in a network based on source and destination link layer addresses.

25 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of McNeill with those of Bots and determine a source and destination from link layering addressing as another means to determine the source and destination of a data packet in order to make sure it is operating within a virtual private network group.

Art Unit: 2137

Claims 4,13,21,30,38, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of Yuasa, U.S. Patent No. 6,085,238.

As per claims 4,13,21,30,38, and 47, the applicant discloses the method of claims 1,12,18,29,35, 5 and 46, which are met by Bots (see above), with the following limitation which is met by Yuasa:

Wherein said incoming PCS is encoded in a header of said first data packet, and wherein said determining comprises decoding said incoming PCS from said header of said first data packet (Yuasa: Col 25, line 53 to Col 26, line 3 and Bots: Fig 6);

Bots discloses the idea that a packet's source and destination addresses are sent in the header 10 of a packet and a receiving VPNU extracts the source and destination addresses and looks up the particular group which corresponds with the addresses in the header. For example, in Bots system if the source address is "A" and the destination address is "B", the VPNU extracts the header information and uses the lookup table to determine that "A" and "B" can communicate with each other and are in "group 15 1". What Bots' system fails to describe is the use of sending "group 1" in the header instead of "A" and "B".

Yuasa discloses a virtual local area network system for communicating information between user groups. Yuasa also discloses the idea of encoding a group ID or PCS into the header information of the packet through the use of a coded tag which identifies the particular group the packet is in. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of 20 Yuasa with those of Bots and incorporate the use of encoding the PCS into the header of the data packet because doing so would be an efficient way to communicate to the VPNU which group the packet is in so the VPNU can either process the packet immediately or make a quick check to authenticate that the group the packet says it is in is really the packet it is in.

25 Claims 14,17,31,34,48, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of Kisor, U.S. Patent No. 6,266,773.

Art Unit: 2137

As per claims 14,17,31,34,48, and 51, the applicant describes the method of claims 13,12,30,29,47, and 46, which are met by Bots (see above), with the following limitation which is met by Kisor:

Further comprising recording an event corresponding to said first data packet in response to 5 detecting said outgoing PCS is not a subset of said destination community set (Col 3, lines 42-67);

Bots discloses all the limitations of claims 13,12,30,29,47, and 46. However, Bots fails to disclose the use of recording an event in a security log. The use of a security log for recording an event is disclosed by Kisor in a computer security system.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to 10 incorporate the ideas of Kisor with those of Bots and add a security log for recording an event for extra security and monitoring in the system.

Any inquiry concerning this communication or earlier communications from the examiner should 15 be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

20 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) 25 at 866-217-9197 (toll-free).



ANDREW CALDWELL  
SUPERVISORY PATENT EXAMINER